REMARKS

Applicants appreciate the Examiner's thorough consideration provided the present application. Claims 1-5 are now present in the application. Claim 1 has been amended. Claim 1 is independent. Reconsideration of this application, as amended, is respectfully requested.

Interview with the Examiner

A telephone interview was conducted with the Examiner in charge of the above-identified application on October 4, 2007. Applicants greatly appreciate the courtesy shown by the Examiner during the interview.

In the interview with the Examiner, Applicants' representative presented arguments with regard to the rejection under 35 U.S.C. §§ 102 and 103. Specifically, it was argued that Schwan fails to teach each and every element recited in claim 1. The Examiner during the interview stated that if claim 1 is amended to recite "[a] method of protecting a cryptographic algorithm (6) before introduction in a device (1) comprising programmable processor unit (4)", the current rejections will be overcome.

In this Reply, claim 1 has been amended as the Examiner suggested, as described hereinbelow.

Claim Rejections Under 35 U.S.C. §§ 102 & 103

Claims 1-3 [sic., 1-4] stand rejected under 35 U.S.C. § 102(b) as being anticipated by Schwan, U.S. Patent Application Publication No. US 2004/0187035. Claim 5 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Schwan in view of Schneier's non-patent publication. These rejections are respectfully traversed.

As mentioned, independent claim 1 has been amended as the Examiner suggested during the interview. In particular, independent claim 1 has been amended to recite "[a] method of protecting a cryptographic algorithm (6) before introduction in a device (1) comprising programmable processor unit (4), the algorithm being separable into the form of initial polynomials (P_i) of at least two variables each, and having a degree of not less than two, the method comprising the steps of providing combined polynomials (Q_k) each obtained from at least two initial polynomials (P_i, P_{i+1}), and of implementing the combined polynomials (Q_k) in the programmable processor unit (4)." Applicants respectfully submit that the above combination of elements as set forth in amended independent claim 1 is not disclosed nor suggested by the references relied on by the Examiner.

In particular, the present invention relates to a method for protecting an algorithm. In the present invention, the algorithm is separated into initial polynomials of at least two variables each, and has a degree of not less than two. At least two initial polynomials are then combined into combined polynomials, and the combined polynomials are implemented in a programmable processor unit.

The present application on page 5, lines 22-30 of the specification states that when the invention is implemented with a DES algorithm, it is then necessary to combine more than two initial polynomials. However, this does not mean that it was known to combine initial polynomials of a DES algorithm and to implement the combined polynomials as the Examiner alleged on page 3, lines 3-5 of the outstanding Office Action.

Schwan discloses the use of a DES algorithm for proceeding to an authentification of a user. For determining the authentification data to which a hacker cannot have access, he tries to modify the algorithm and/or vary the data submitted to the algorithm, and he observes the corresponding variations when the algorithm is implemented. Schwan does not suggest to protect the algorithm **before** it is introduced in a device but when it is implemented in the device. To this effect Schwan combines two features (see Schwan, paragraphs 7 and 8): an encapsulation of the algorithm and a control of access to the data input. Those features have nothing in common with the method of separating the algorithm into initial polynomials and combining them for safe transport.

With regard to the Examiner's reliance on Schneier, this reference also fails to disclose the above combination of elements as set forth in amended independent claim 1. Accordingly, this reference fails to cure the deficiencies of Schwan.

Accordingly, neither of the references utilized by the Examiner individually or in combination teaches or suggests the limitations of amended independent claim 1 or its dependent claims. Therefore, Applicants respectfully submit that claim 1 and its dependent claims clearly define over the teachings of the references relied on by the Examiner.

Accordingly, reconsideration and withdrawal of the rejections under 35 U.S.C. §§ 102 and 103 are respectfully requested.

CONCLUSION

Since the remaining patents cited by the Examiner have not been utilized to reject the claims, but merely to show the state of the prior art, no further comments are necessary with respect thereto.

It is believed that a full and complete response has been made to the Office Action, and that as such, the Examiner is respectfully requested to send the application to Issue.

In the event there are any matters remaining in this application, the Examiner is invited to contact Joe McKinney Muncy, Registration No. 32,334 at (703) 205-8000 in the Washington, D.C. area.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicants respectfully petition for a one (1) month extension of time for filing a response in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§1.16 or 1.17; particularly, extension of time fees.

Dated: October 15, 2007

Respectfully submitted,

By____________________
for Joe McKinney Muncy
Registration No.: 32,334 #43,368
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant